REMARKS

Applicant respectfully requests review of this application. Claims 1-28 are currently pending.

No claims are amended. No claims have been cancelled or added.

Thus, claims 1-28 are hereby presented for examination.

Claim Rejection under 35 U.S.C. §112

The Examiner rejected claims 6, 11 and 21 under 35 U.S.C. 112, second paragraph, as failing to particularly point out and distinctly claim the subject matter. Specifically the Office Action refers to the limitation "the group" in the rejected claims.

It is respectfully submitted that the current claims are in the correct legal form, and should not be modified. The three rejected claims each recite a Markush group, and the "the group" is part of the accepted language, as provided in the *In re Markush* decision. "A Markush-type claim recites alternatives in a format such as 'selected from the group consisting of A, B and C.' See Ex parte Markush, 1925 C.D. 126 (Comm'r Pat. 1925)." (MPEP, § 803.02) (emphasis added)

It is submitted that, based on the acceptance of the claim format judicially, the Markush claim format contained in claims 6, 11, and 21 cannot be rejected. "The group" is the correct legal form for this type of claim, and the rejection of claims 6, 11, and 21 thus must be removed.

Claim Rejection under 35 U.S.C. §103

TPM and TCG

Claims 1-28 were rejected under 35 USC §103 (a) as being unpatentable over Trusted Platform Module – White Paper (hereinafter referred to as "*TPM*") in view of *Applied Cryptography* and TCG Main Specification Version 1.1a (hereinafter referred to as "*TCG*").

While the main reference for the rejection is *TPM*, Applicant is not certain what this document is. It does not appear that this document has been identified by the Examiner and it does not appear that this reference has been cited by the Applicant.

The Applicant searched the Internet and did find a document entitled "Trusted Platform Module (TPM) Based Security on Notebook PCs – White Paper", Sandeep Bajikar, June 20, 2002. It appears that this document may be *TPM* cited by the Office Action as the citations in the Office Action appear to relate to this document. In order to move prosecution of the claims forward, the Applicant is assuming that this is the correct document, and is proceeding on this basis. However, Applicant requests clarification of the rejection and identification of the prior art that is being cited.

Claim 1 is again as follows:

1. A method comprising:
   requesting a service for a platform from a service provider;
   receiving a service key request for the service from the service provider, wherein the service key is to be limited to one or more acceptable configurations of the platform;

generating a service key pair that is limited to the one or more acceptable configurations of the platform, and returning a public key of the key pair to the service provider;

certifying the use of the service for the one or more acceptable configurations of the platform; and

receiving a session key for a session of the service from the service provider, the service being limited to the one or more acceptable configurations of the platform.

The claim thus includes "receiving a service key request for the service from the service provider, wherein the service key is to be limited to one or more acceptable configurations of the platform", "generating a service key pair that is limited to the one or more acceptable configurations of the platform", "certifying the use of the service for the one or more acceptable configurations of the platform" and "the service being limited to the one or more acceptable configurations of the platform". It is respectfully submitted that the cited references do not teach or reasonably suggest these claim limitations.

The Office Action indicates that *TPM* "does not disclose the public key (service key) being bound to one or more configurations of the platform or exchanging a session key." This does not precisely follow the language of the claim, but Applicant understands this to mean that *TPM* thus does not provide for "receiving a service key request for the service from the service provider, wherein the service key is to be limited to one or more acceptable configurations of the platform", "generating a service key pair that is limited to the one or more acceptable configurations of the platform", "certifying the use of the service for the one or more acceptable configurations of the platform" and "the service being limited to the one or more acceptable configurations of the platform". (Claim 1) (emphasis added)

The Office Action indicates that *TCG* discloses a command (TPM_Seal) "that stores a secret key to a configuration of the platform configuration registers." It is respectfully submitted that the suggested operation is not relevant to the claim elements at issue. The TPM_Seal operation is one of a number of processes by which a TPM protects confidential data. "This section introduces the processes by which a TPM may act as the portal to confidential data stored on arbitrary storage media." (*TCG*, §7, p. 145) This thus is not related to the provision of services, but rather to the unlocking of secrets. As a part of the protection of secrets, the TPM_Seal command allows for the concatenation of additional information to "seal" the confidential data. As described in the specification, the Bind command and the Seal command are described as follows:

> TSS_Bind: External data is encrypted under a parent key. (TPM_UnBind decrypts the blob using the parent key and exports the data from the TPM.)
>
> TPM_Seal: External data is concatenated with a value of integrity metric sequence and encrypted under a parent key. (TPM_Unseal decrypts the blob using the parent key and exports the plaintext data if the current integrity metric sequence inside the TPM matches the value of integrity metric sequence inside the blob). The sealer of the data may specify that no integrity metrics are required.

(*TCG*, §7, p. 146) Thus, in general the difference between the binding operation and the sealing operation is that in the latter case the external data is concatenated with "a value of integrity metric sequence".

This is further explained in section 7.2.1 of *TCG*, which describes the command in detail and indicates that:

> The SEAL operation allows software to explicitly state the future "trusted" configuration that the platform must be in for the secret to be revealed. The SEAL operation also implicitly includes the relevant platform configuration (PCR-values) when the SEAL operation was performed. The SEAL operation uses the tpmProof value to BIND the blob to an individual TPM.

(*TCG*, §7.2.1, p. 151) Thus, in this operation, there is an additional assurance that a particular "trusted configuration" is present in order for a secret to be revealed. The reason this is done is to provide assurance of the platform that is seeking the confidential data:

> For example, if SEAL is used to store a secret key for a future configuration (probably to prove that the platform is a particular platform that is in a particular configuration), the only requirement is that that key can be used only when the platform is in that future configuration. Then there is no interest in the platform configuration when the secret key was SEALed. An example of this case is when SEAL is used to store a network authentication key.

(*TCG*, §7.2.1, p. 151) Thus, seal does provide additional identify information that is tied to the configuration of the platform when the confidential information is requested.

However, in an attempt to analogize the cited reference to the claims here (ignoring other differences between the claims and the references), the command in the *TCG* reference only limits who can get the confidential information – it does nothing to limit where the information is used. Once the confidential information is available, the reference does not address the use of the data, or, in particular, the configuration of the platform in which the data might be used.

The claim limitations that are at issue are not directed to simply obtaining confidential data, as are the cited portions of the *TCG* reference, but rather to generating a service key pair that is limited to the one or more acceptable configurations of the platform, certifying the use of the service for the one or more acceptable configurations of the platform, and providing service that is limited to the one or more acceptable configurations of the platform.

Thus, it is submitted that the cited portion of *TCG* is not relevant to service keys that are limited to one or more configurations because the claims regard limiting operations to the one or more configurations, something that the TPM_Seal does not do and does not contemplate – the use of services is not discussed in the reference. The limitations provided in claim 1 are not shown in this reference.

The Office Action also cites to *Applied Cryptography* as disclosing "a hybrid cryptosystem that is used to exchange a session key by using public key cryptography." This concept does appear to be discussed in this reference, but again this is only relevant to limiting the access to the session key, which again is a question of protecting confidential data and ensuring only authorized persons obtain such data. This does not address the limitation of the use of the session key – the session key would apparently be usable under any configuration of a platform.

Thus, the cited references, separately or in combination, do not teach or reasonably suggest all of the elements of claim 1.

It is submitted that the arguments presented above with regard to claim 1 are also applicable to independent claims 8, 13, 16, 23, and 26.

The remaining rejected claims, while having other differences with the cited references, are dependent claims, and are allowable as being dependent on the allowable base claims.

Conclusion

Applicant respectfully submits that the rejections have been overcome by the amendment and remark, and that the claims as amended are now in condition for allowance. Accordingly, Applicant respectfully requests the rejections be withdrawn and the claims as amended be allowed.

Invitation for a Telephone Interview

The Examiner is requested to call the undersigned at (503) 439-8778 if there remains any issue with allowance of the case.

Request for an Extension of Time if Needed

The Applicant respectfully petitions for extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. § 1.136(a) should one be needed. Please change the fee under 37 C.F.R. § 1.17 for such extension to our Deposit Account No. 02-2666.

Charge our Deposit Account

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: March 21, 2008

/Mark C. Van Ness/
Mark C. Van Ness
Reg. No. 39,865

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(503) 439-8778